



DEPARTMENT OF THE NAVY

COMMANDER NAVY REGION SOUTHWEST
937 NO. HARBOR DR.
SAN DIEGO, CALIFORNIA 92132-0058

IN REPLY REFER TO:

COMNAVREGSWINST 5511.1

N6R

16 Aug 04

COMNAVREGSW INSTRUCTION 5511.1

Subj: EMERGENCY ACTION PLAN (EAP) FOR PROTECTION OF ELECTRONIC
KEY MANAGEMENT SYSTEM (EKMS) MATERIAL

Ref: (a) SECNAVINST 5510.36
(b) CMS 21
(c) COMNAVREGSWINST 2280.1

Encl: (1) Emergency Protection Procedures
(2) Emergency Removal Procedures
(3) Emergency Destruction Priorities
(4) Sample Message Report

1. Purpose. To promulgate instructions and information regarding actions to be taken to prevent classified and cryptographic information and materials from unauthorized disclosure at Commander, Navy Region Southwest ((COMNAVREG SW), during emergency situations, per references (a) through (c).

2. Scope. The ultimate reason for all security measures is to prevent unauthorized access to classified and cryptographic information. The possibility of unauthorized access is increased during times of emergency. It is necessary, therefore, that procedures be in place to deal with an emergency situation.

3. Responsibilities. The Electronic Key Management System (EKMS) Manager is responsible for the security and effective operation of the COMNAVREG SW EKMS account, administrative coordination of this plan and the accuracy of this instruction. The EKMS Manager shall ensure that all assigned COMNAVREG SW personnel who handle COMSEC material are trained in the actions required in the event this plan or portions thereof are executed. The Staff CMS Responsibility Officer (SCMSRO) is responsible for the implementation of this plan. Should conditions prevent contact with the SCMSRO, the Regional Information Technology Service Center (RITSC) Information Assurance (IA) Director, EKMS Manager, or senior person present, in that order, is empowered to implement the appropriate emergency plan to be conducted by COMNAVREG SW personnel.

16 Aug 04

4. Background. The Electronic Key Management System (EKMS) is an interoperable collection of systems developed by services and agencies of the U.S. Government to automate the processing of electronic key and management of other types of Communications Security (COMSEC) material. Each department holding or using COMSEC material, including Secure Telephone Unit Third Generation (STU-III), must prepare a plan for the protection of the material in emergency situations. Per Exhibit 2B of reference (a) and Annex M of reference (b), activities within the 48 contiguous states are not required to include emergency destruction in the EAP. Emphasis, instead, will be placed on the protection of material in a natural disaster or apparent short-lived civil uprising. During these emergencies, planning and action shall be directed toward maintaining security control over the material until the emergency has passed:

a. During an emergency, the senior individual present must determine whether securing, removing, or destroying will best protect the material on hand. To minimize the actions required to protect COMSEC material, only the minimum amount of such material shall be held at any time; the material shall be stored to facilitate emergency removal or destruction; routine destruction will be conducted frequently to dispose of superseded and/or unnecessary material as directed by appropriate authorities.

b. There are two types of emergencies that may arise: natural disaster and hostile action. A **natural disaster** includes such things as fire, flood, tornado, earthquake, lightning strike, etc. A **hostile action** includes enemy attack, sustained civil disturbance, and terrorism.

(1) During natural disaster emergencies the risk of an attempt by hostile forces to capture classified and/or cryptographic materials is extremely low. Planning and actions therefore, should be focused on maintaining control over the material until the emergency has passed.

(2) In the case of a hostile action emergency, the assumption must be made that the classified and/or cryptographic material is the target. Planning and actions must be focused on keeping the material from unauthorized persons, whether they are enemy troops, rioters, terrorists, or other.

(3) When an emergency occurs, there are three courses of action possible for the protection of COMSEC material:

(a) Emergency Protection/Securing. In the event of a natural disaster or civil riot of short duration, classified material shall be stored in authorized containers. If feasible, an armed guard shall be posted near the containers. If the area must be evacuated, a complete inventory shall be taken upon return to the area to determine what, if any material is missing. Procedures are outlined in enclosure (1).

(b) Emergency Removal. Emergency removal will be conducted only when directed by appropriate authority. In the event of a fire, major civil riot or other emergency situations, it may become necessary for classified and COMSEC material to be removed by uncleared personnel. In this case, the removal must be under the complete and continuous supervision of authorized personnel. In the case of a fire, any attempt at removal must be made simultaneously with efforts to extinguish and control the fire. The removal should not interfere with firefighting efforts or subject personnel to unnecessary danger. Removal of the material should be coordinated in such a manner that the EKMS Manager knows the location of the material at all times. Removal procedures are outlined in enclosure (2).

(c) Emergency Destruction. Emergency destruction actions include: partial precautionary destruction and complete emergency destruction. When a possible emergency is foreseen, it is highly desirable that action be taken to reduce the amount of classified cryptographic information and material held to the minimum essential to effect operations should it become necessary. Destroying the material should be considered as the absolute last alternative. All reasonable efforts should be made to secure or remove the material. The senior person present will determine the method of destruction to be used depending upon the situation. Upon direction of competent authority, the senior person present will implement and carry out the emergency destruction of COMSEC material in accordance with the destruction priorities listed in enclosure (3). **Only authorized persons** must destroy COMSEC material. A record of all COMSEC material destroyed will be maintained and presented to the senior person present upon completion of destruction. Partial precautionary and complete emergency destruction priorities and procedures are listed in enclosure (3). One or more of the following methods will be used to destroy COMSEC and other classified material:

1. Burning. The individual responsible for destruction should ensure that all documents are disassembled and crumpled individually, if possible, as thick documents in

book form do not burn completely. The material must then be delivered to a pre-designated area and burned in trash receptacles. A record of material burned while conducting destruction shall be maintained. All burn residue should be thoroughly checked to ensure complete destruction.

2. Shredding/Disintegration. Only paper material is authorized for shredding. Paper material that is shredded must be no larger than 5 mm. Key tape must be destroyed by burning or disintegration. If a disintegrator is not available, key tape may be shredded and the residue burned. A record of material shredded/disintegrated while conducting destruction shall be maintained. The shredded/disintegrated material must be checked periodically during the destruction process to ensure complete destruction.

(d) In case of imminent capture, focus on destroying as much material as time permits following the emergency destruction priorities in enclosure (3), paragraph 4c.

5. Action. Upon learning of possible implementation of the Emergency Action Plan, the senior person present shall notify the SCMSRO, RITSC IA Director, and EKMS Manager. Immediately recall personnel needed to accomplish an emergency destruction (see enclosure (3)). Emergency destruction of classified material and equipment should not be implemented when simply removing or securing the material would afford the protection and security required. Should competent authority decide to implement removal or securing of COMSEC material, the senior person present will notify the SCMSRO when the appropriate plan has been completed.

a. Reporting Destruction. Accurate information relative to the extent of an emergency is absolutely essential to the effective evaluation of the COMSEC impact of the occurrence, and second in importance only to the conduct of thorough destruction. The SCMSRO and EKMS Manager are responsible for reporting the attendant facts of the emergency to the appropriate seniors in the chain of command by the most expeditious means available.

(1) External Reporting Instructions: The initial destruction report and all amplifying reports shall be forwarded via record message to the following addresses:

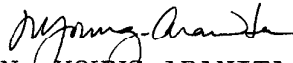
CNO WASHINGTON DC//N09N2/N643//
CNI WASHINGTON DC//N6//
COMNAVNETWARCOMNORFOLK VA//N6//
COMNAVNETSPAOPSCOM DAHLGREN VA//N6//
DMCS WASHINGTON DC//N5//
DIRNSA FT GEORGE G MEADE MD//I413/Y13//

16 Aug 04

and both operational and administrative command echelons as soon as possible. If feasible, use a secure means of reporting. See enclosure (4) for sample messages.

(2) Required Information: State in the report the material destroyed, the method and extent of destruction, and any classified COMSEC material items presumed to have been compromised, i.e., not destroyed or not completely destroyed. (Note: If feasible, follow the reporting procedures for COMSEC Incidents as outlined in Exhibit 2B of reference (a) and Chapter 9 of reference (b)).

b. Training. Emergency Action Plan drills will be conducted and documented at least annually to ensure that everyone, especially newly assigned personnel who might have to take part in an actual emergency, will be able to carry out their duties, and to determine if the present plan is adequate, workable, and up-to-date.


N. YOUNG-ARANITA
By direction

Emergency Protection Procedures

1. Emergency plans provide for the protection of classified information in a way that will minimize the risk of personal injury or loss of life. For instance, in the case of a fire, the senior on-scene person should order the immediate evacuation of personnel at risk and not require that all classified information be properly stored prior to evacuation. A perimeter guard or controlling access to the area will provide sufficient protection without endangering personnel. In the event of fire that threatens COMSEC material, the person(s) discovering the fire shall:

a. Sound the alarm (make others aware of the fire); call 9-911 to report the fire. If needed, request fire-fighting assistance and have someone direct firefighting personnel to the scene.

b. Ventilation and electrical power shall be secured to the affected area

c. Notify the SCMSRO AND EKMS Manager immediately. The senior person present will assign cleared personnel on-the-scene responsibility for protecting COMSEC material. Protect COMSEC material, as much as possible, from unauthorized disclosure, when admitting outside fire fighters into the secure area(s). If feasible, secure the material in approved containers. All efforts at protecting the material must be made simultaneously with efforts to extinguish and control the fire, and should not interfere with fire-fighting efforts or subject personnel to unnecessary danger.

d. When the fire has been extinguished, authorized personnel will conduct a complete inventory to determine what material was damaged or lost in the fire. Assess and report the probable exposure of classified COMSEC material to unauthorized persons during the emergency.

e. A report of all the facts surrounding the emergency will be forwarded to both the administrative and operational command echelons as soon as possible. The report shall be sent by secure means and should identify the material destroyed, the method and extent of destruction, and any classified/COMSEC material presumed to have been compromised. The report shall be formatted per enclosure (4).

16 Aug 04

Emergency Removal Procedures

1. Flood/Natural Disaster. In the event of flood, earthquake, hurricane, or other natural disaster, which threatens or compromises the integrity of COMSEC area(s), the material shall be moved to safer storage and handled in the following manner:

a. If feasible, COMSEC material will be moved to safer storage (i.e., Naval Computer and Telecommunications Station (NAVCOMTELSTA), San Diego, Automated Technical Control Facility (ACTF), located at the far southwest end of Building 1482, by the warehouse ramp, or in the Building 825, Naval Base Coronado, COMSEC vault). Notify the NAVCOMTELSTA San Diego Communications Watch Officer (CWO) at (619) 545-6983 that you will be bringing COMSEC material for safe storage until the emergency has past. Ensure that a list is made of all the material moved to safe storage. During transit, particular attention shall be given to the prevention of damage, loss, and unauthorized disclosure. COMSEC material must be moved in a covered vehicle. Open pick-up trucks, stake trucks etc., are strictly prohibited.

b. When moving the Key Processor (KP) to safe storage, it shall be covered and protected as SECRET material. The unkeyed KP is SECRET because as a key generator/processor, handling bulk keying material, it is much more sensitive than normal COMSEC equipment. The KP is sensitive to sudden movement and jarring and should be handled with the utmost of care.

c. Take the Local COMSEC Management Software (LCMS) hard drive and latest backup tape with the KP to the safe storage facility.

d. Immediately after the danger has passed, authorized personnel will conduct a complete inventory to determine what material was damaged or lost and file a report as directed by references (a) and (b). The report format is delineated in Enclosure (4).

16 Aug 04

Emergency Destruction Priorities

1. This plan has three different Destruction Priority lists: Precautionary destruction List A, complete destruction List B, and complete destruction List C. When personnel and/or destruction facilities are limited, join the three categories and destroy the material following the priorities listed in Priority List C. Precautionary destruction should be a matter of daily routine. Maintaining COMSEC material to the minimum essential requirements will greatly reduce the time required to destroy material in an emergency.

2. In case of an apparent short-lived civil uprising when the facility may be temporarily abandoned, destroy all superseded COMSEC keying material by shredding or burning in waste receptacles. (Record all material destroyed for formal report.)

3. In case of a sustained civil uprising, mob or terrorist action, or enemy attack, implement and carry out emergency destruction of COMSEC material. Any of the methods approved for routine destruction may be used for emergency destruction. Printed matter must be destroyed beyond reconstruction. COMSEC equipment must be rendered inoperable i.e., beyond reuse. If time permits remove and destroy classified circuit boards and multi-layer boards. If these elements are destroyed, it is not necessary to destroy the remainder of the equipment. Maintain an accurate list of all destroyed material for the required formal reports.

4. When directed by appropriate authority, the senior person present shall initiate destruction procedures using one of the following destruction priorities, as the situation dictates:

a. **Precautionary Destruction Priority List A.** When destruction priority List A is used, destroy COMSEC material in the following order:

(1) All superseded keying material.

(2) TOP SECRET primary keying material.

(3) SECRET, CONFIDENTIAL, and UNCLASSIFIED primary keying material.

Enclosure (3)

16 Aug 04

(4) Non-essential classified maintenance, operating, and administrative manuals.

b. **Complete Destruction Priority List B.** When sufficient personnel and facilities are available, destroy COMSEC material in the following order:

(1) All superseded COMSEC keying material.

(2) Effective keying material, including key variables stored electrically in crypto equipment and fill devices.

(3) If held, Reserve-on-Board (ROB) material that will become effective within 30 days.

(4) All remaining classified material.

(5) Make a reasonable effort to evacuate COMSEC equipment, but the immediate goal is to render them unusable and beyond reconstruction. Although it is desirable to destroy jeopardized crypto-equipment so thoroughly that logic reconstruction is impossible, this cannot be guaranteed in most environments. In this case, the following procedures apply:

(a) Zeroize FASTLANES, TACLANES, STU-IIIs, KIV-7s, KP, DMDs, DTDs and other fill devices.

(b) Remove KP motherboard and destroy by incineration.

(c) Remove and destroy readily removable classified elements (e.g., printed circuit cards, LCMS hard drive and backup tapes, etc.).

c. **Complete Destruction Priority List C.** In cases where personnel and facilities are limited, destroy COMSEC material in the following order:

(1) All superseded and currently effective COMSEC keying material, regardless of its classification, including key variables stored electrically in crypto equipment and fill devices.

(2) Zeroize FASTLANES, TACLANES, STU-IIIs, KIV-7s, KP, DMDs, DTDs and other fill devices.

(3) If held, ROB material.

16 Aug 04

- (4) Remove KP motherboard and destroy by incineration.
- (5) Remove and destroy LCMS hard drive and backup tapes.
- (6) Remaining classified publications and documents.
- (7) Classified elements of COMSEC equipment.
- (8) Destroy all or as much COMSEC equipment as time will permit.

16 Aug 04

1. Initial Destruction Report. Notify appropriate authorities upon commencement of emergency destruction. If feasible the message should be sent via secure means (SIPRNET, STU-III, Secure Termination, etc.). A secure voice report to the appropriate authorities, followed later by a message report should suffice. The following is a sample of an initial notification report:

Sample Message Reports

******* S A M P L E MESSAGE *******
******* CLASSIFIED FOR TRAINING PURPOSES ONLY *******

ZTTCZYUW RUWDHLP0001 2031900-CCCC-RUWDHLP RHMCSUU.
ZNR CCCCC
Z 221900Z JUN 04
FM COMNAVREG SW SAN DIEGO CA//00/N6//
TO CNO WASHINGTON DC//N09N2/N643//
CNI WASHINGTON DC//N6//
COMNAVNETWARCOM NORFOLK VA//N6//
COMNAVNETSPAOPSCOM DAHLGREN VA//N6//
HQ PACOM HONOLULU HI//J63//
DIRNSA FT GEORGE G MEADE MD//I413/Y13//
DCMS WASHINGTON DC//N5//
AIG 11056
BT
C O N F I D E N T I A L //N02280//
MSGID/GENADMIN/COMNAVREG SOUTHWEST//
SUBJ/EMERGENCY DESTRUCTION OF COMSEC MATERIAL//
REF/A/DOC/DCMS/09JUN2000//
AMPN/CMS 21A//
RMKS/1. (C) COMNAVREG SOUTHWEST EKMS ACCOUNT 151016 IS COMMENCING
EMERGENCY DESTRUCTION OF COMSEC MATERIAL ON HAND DUE TO IMPENDING
TERRORIST OVERRUN OF EKMS FACILITIES AT NAVAL BASE CORONADO,
CALIFORNIA.//
DECL/X1//
BT
#0001
NNNN

THIS PAGE IS UNCLASSIFIED.
ABOVE MESSAGE CLASSIFIED FOR TRAINING PURPOSES ONLY.

Enclosure (4)

COMNAVREGSWINST 5511.1

16 Aug 04

2. Interim/Amplifying/Final Report. It is absolutely essential that the controlling authorities of keying material know, as soon as possible, what material has been subjected to unauthorized disclosure. Where time and facilities permit, amplifying messages should be sent to inform all concerned of the progress of the emergency destruction. A final report must be sent identifying the status of all COMSEC material involved.

***** S A M P L E MESSAGE *****

***** CLASSIFIED FOR TRAINING PURPOSES ONLY *****

OTTCZYUW RUWDHLP0001 2031901-CCCC-RUWDHLP RHMCSUU.

ZNR CCCC

O 221901Z JUN 04

FM COMNAVREG SW SAN DIEGO CA//00/N6//

TO CNO WASHINGTON DC//N09N2/N643//

CNI WASHINGTON DC//N6//

COMNAVNETWARCOM NORFOLK VA//N6//

COMNAVNETSPAOPSCOM DAHLGREN VA//N6//

HQ PACOM HONOLULU HI//J63//

DIRNSA FT GEORGE G MEADE MD//1413//

DCMS WASHINGTON DC//N5//

AIG 11056

BT

C O N F I D E N T I A L //N02280//

MSGID/GENADMIN/COMNAVREG SOUTHWEST//

SUBJ/EMERGENCY DESTRUCTION OF COMSEC MATERIAL//

REF/A/RMG/COMNAVREG SW/221900ZJUN2004//

AMPN/INITIAL REPORT COMMENCING EMERGENCY DESTRUCTION OF COMSEC MATERIAL//

RMKS/1. (C) PER REF A, COMNAVREG SOUTHWEST EKMS ACCOUNT 151016 COMMENCED EMERGENCY DESTRUCTION OF ALL COMSEC MATERIAL ON HAND. FOLLOWING MATERIAL PARTIALLY DESTROYED AND/OR SUBJECT TO COMPROMISE DUE TO UNAUTHORIZED DISCLOSURE:

SHORT TITLE	EDITION	SERIAL NUMBERS
AKAA 123	AM	233 - 244
USKAT 4567	MA	233 - 244

2. FOLLOWING MATERIAL HAS BEEN COMPLETELY DESTROYED BY CROSSCUT SHREDDING, SMASHING AND INCINERATION:

SHORT TITLE	EDITION	SERIAL NUMBERS
AKAC 2345	AAB	237 - 244
KAM 111	A	1155
KG175		E21000
USEAD A1234	C//	

DECL/X1//

BT

#0001

NNNN

THIS PAGE IS UNCLASSIFIED.

ABOVE MESSAGE CLASSIFIED FOR TRAINING PURPOSES ONLY.